RSAC 2025 Conference

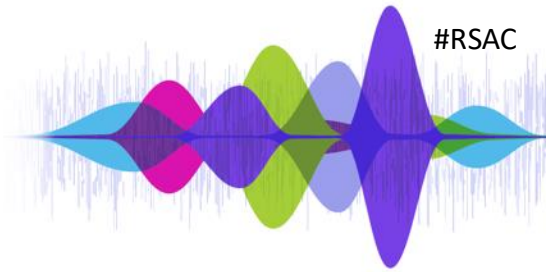
Many Voices.
One Community.

SESSION ID: IMT-M06

# From Snowflake to Snowstorm: Navigating Breaches and Detections

**Roei Sherman**

Senior Director, Research
Mitiga
https://www.linkedin.com/in/freed0m/



# Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

# Roei Sherman

## Senior Director, Resarch @ Mitiga

Ex-Global Director, Offensive Services
AB InBev | Independent IR

B.A - Information systems
and Cybersecurity, M.A - Criminology

Co-organizer of BSidesTLV,
Defcon goon, Trace Labs Volunteer
Judge, Diana's Initiative CFP Staff

Amateur Homebrewer

MITIGA

Adversaries
aren’t breaking in,
**they log in.**

MITIGA

# The Snowflake Campaign – TL;DR

**Threat Actor**

UNC5537

Financially Motivated

**Victims**

165+ Organizations

Santander ticketmaster

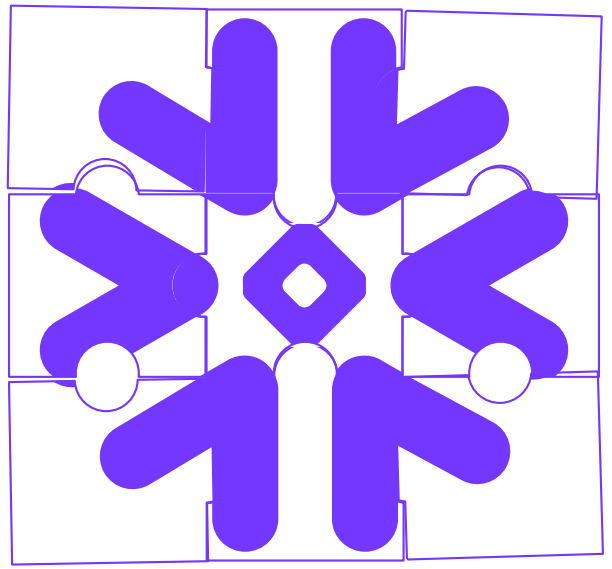
**Time Frame**

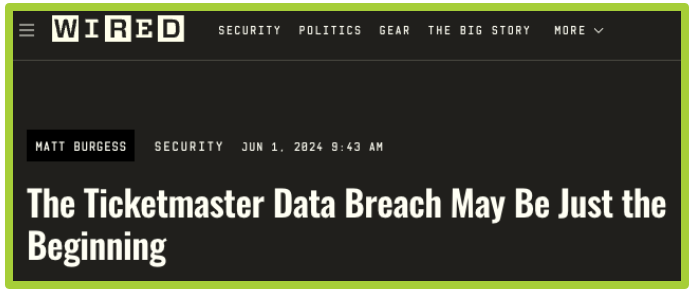
Few Months

**Vulnerability**

None

Combination of Misconfigurations




WIRED
SECURITY POLITICS GEAR THE BIG STORY MORE
MATT BURGESS SECURITY JUN 1, 2024 9:43 AM
The Ticketmaster Data Breach May Be Just the Beginning

# The Snowflake Campaign – ATT&CK

**Exfiltration**

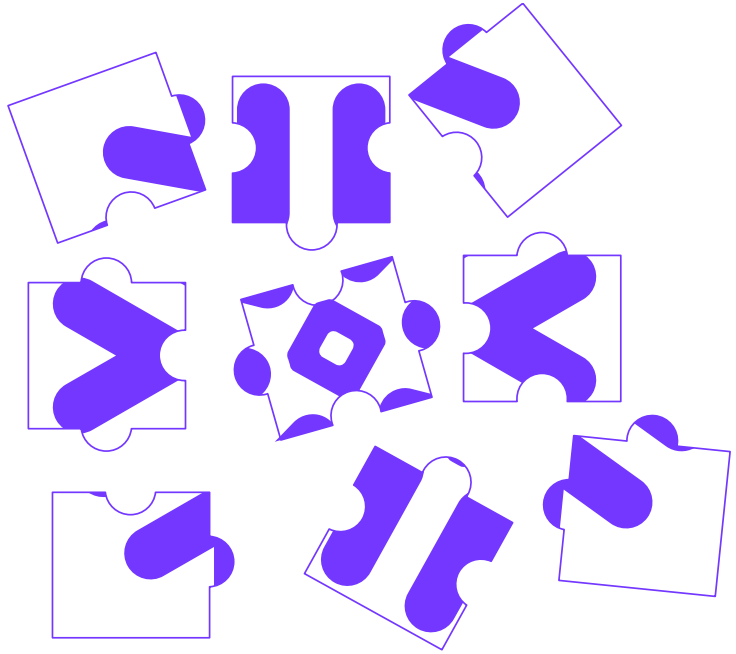
Exfiltrate data outside of the organization

**Resources Development**

Tool to automate the exploitation

Way to identify instances owned by victims

Staging place for stolen data



**Impact**

Extortion

**Initial Access**

Obtain creds from infostealer

Identify snowflake instance (Native tool)

# The Actual Issues

Challenges securing SaaS against identity attacks.

Credentials stolen via infostealer

Accounts lacking MFA

# The Actual Issues

**Built-in Snowflake features to exfiltrate data**

Detecting and mitigating by

**Enforcing MFA and monitoring for unusual activities**

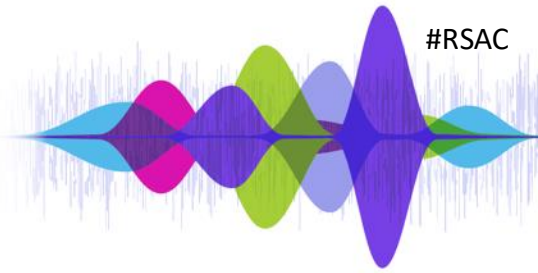
# Could Companies Detect This?

Does SaaS provide security logs?

Are you ingesting them?

Have you investigated them?

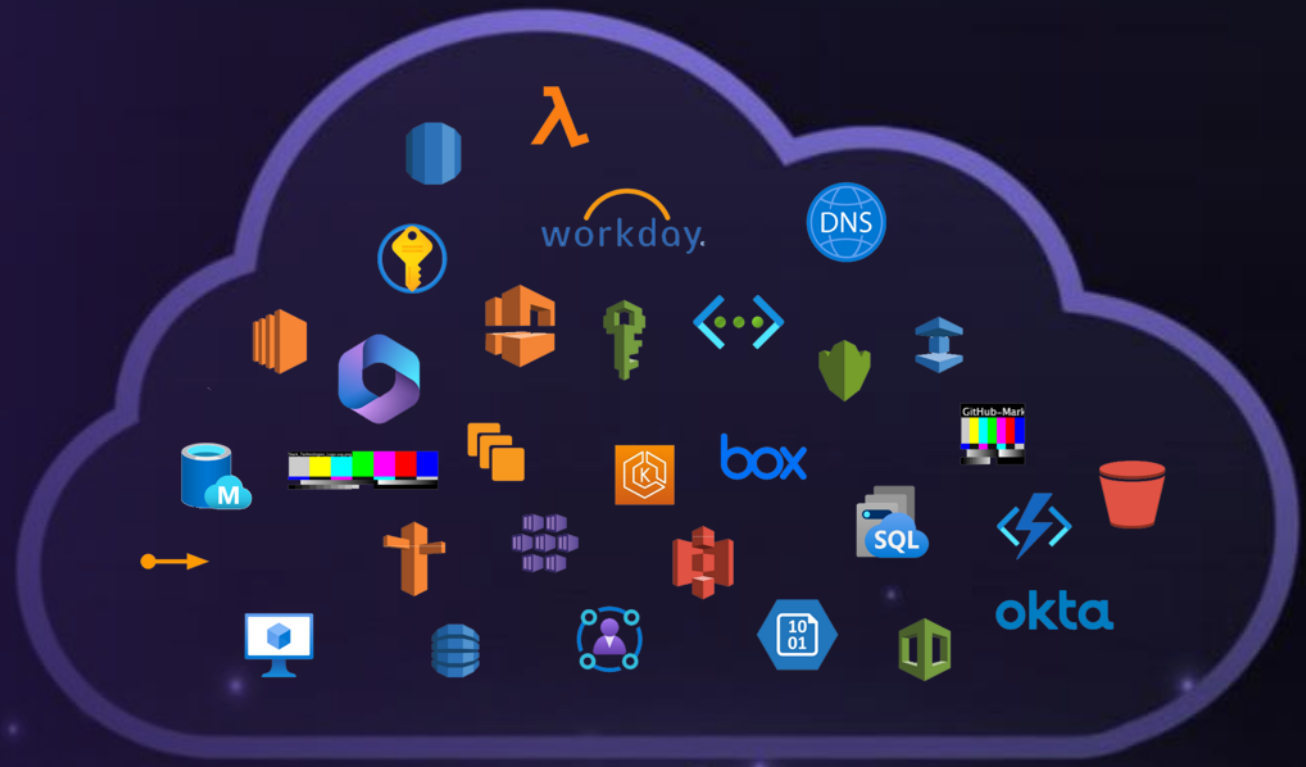
# Could Companies Detect This?



Do you have detection for inner-SaaS actions or just logins?

We must remember,

# SaaS is Cloud.



# Case Study: Midnight Blizzard

**Attacked** November 2023

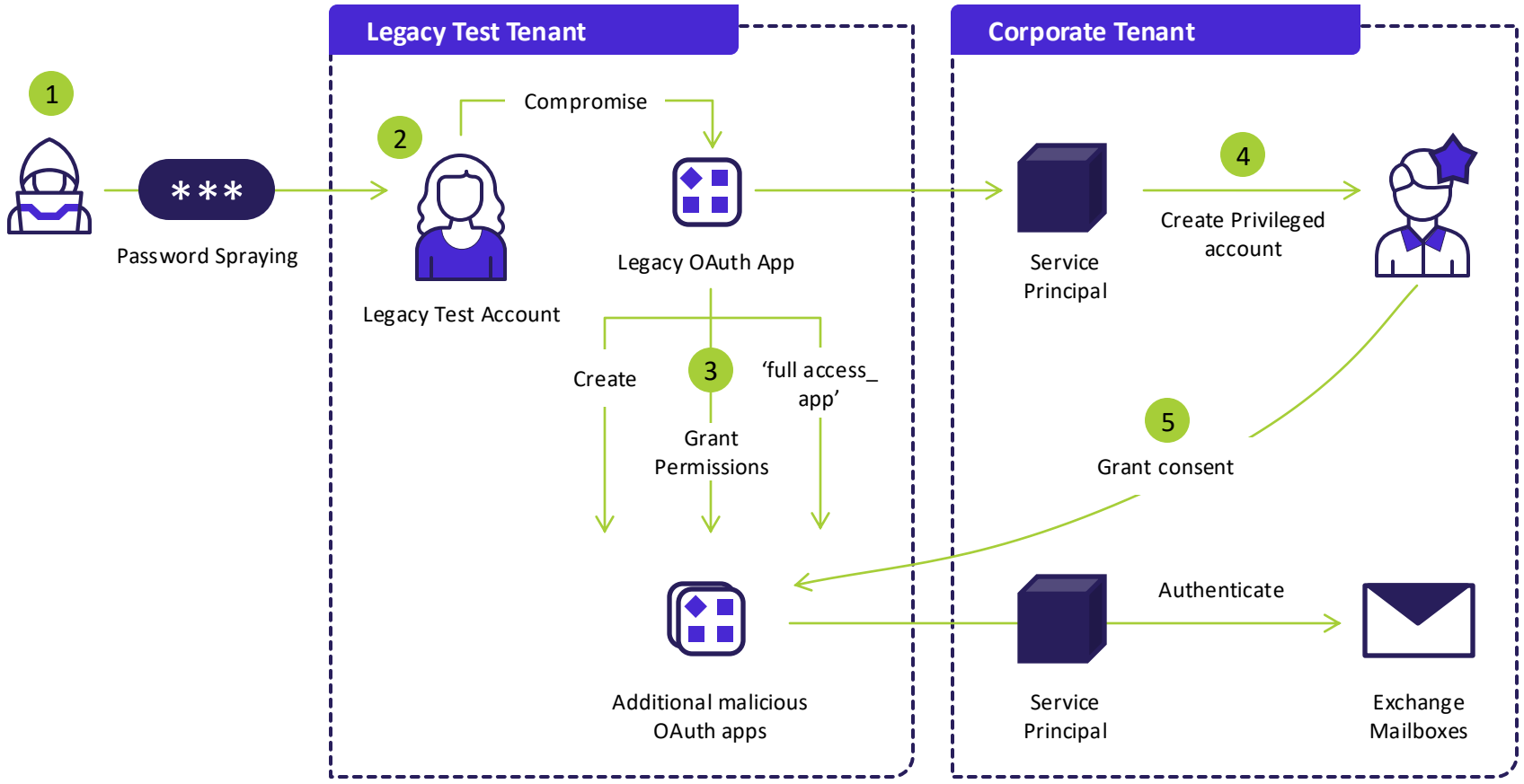
**Disclosed** January 2024

Threat actor is APT

TTPs used are basic and common

Target was Microsoft – owner and builder of Azure – one of the main Cloud Service Providers

## "Guesstimated" Attack Flow




MITIGA

# Cloud Detection Engineering Is HARD

## Context-Aware, Behavioral, and Anomaly-based

Do we have a baseline to compare against actions?

When actions are identical, we need to detect intention.

Should generic logic be be applied across the board?

# Problem 1 : Visibility

## CSP

- Turned off by default
- Retention time, regions
- Log types, log content

## SaaS

- Doesn’t always exist
- License tier
- Security logs vs. application logs

# Solution 1 : Visibility

## CSP

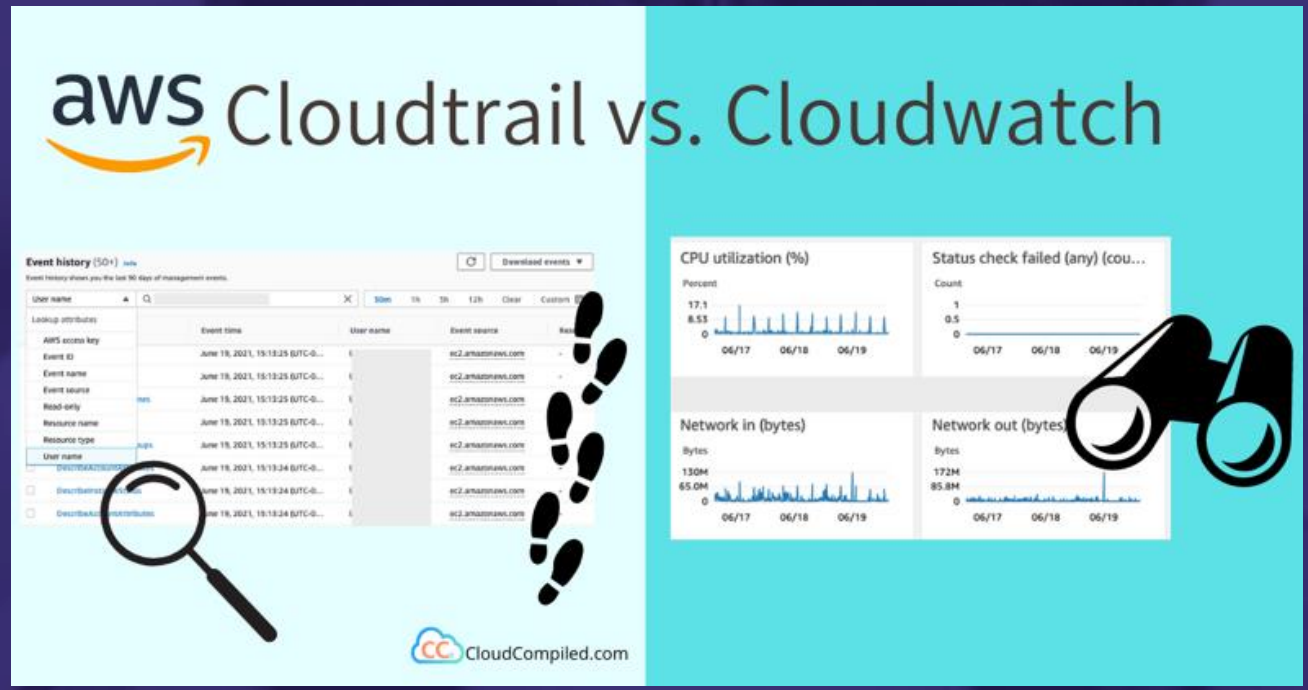
- Turned off by default
- Retention time, regions
- Log types, log content

## SaaS

- Doesn't always exist
- License tier
- Security logs vs. application logs

MITIGA

## Verify DevOps know what to activate



# Solution 1 : Visibility



## CSP

- Turned off by default
- Retention time, regions
- Log types, log content

## SaaS

- Doesn’t always exist
- License tier
- Security logs vs. application logs

MITIGA

# Solution 1 : Visibility

## CSP

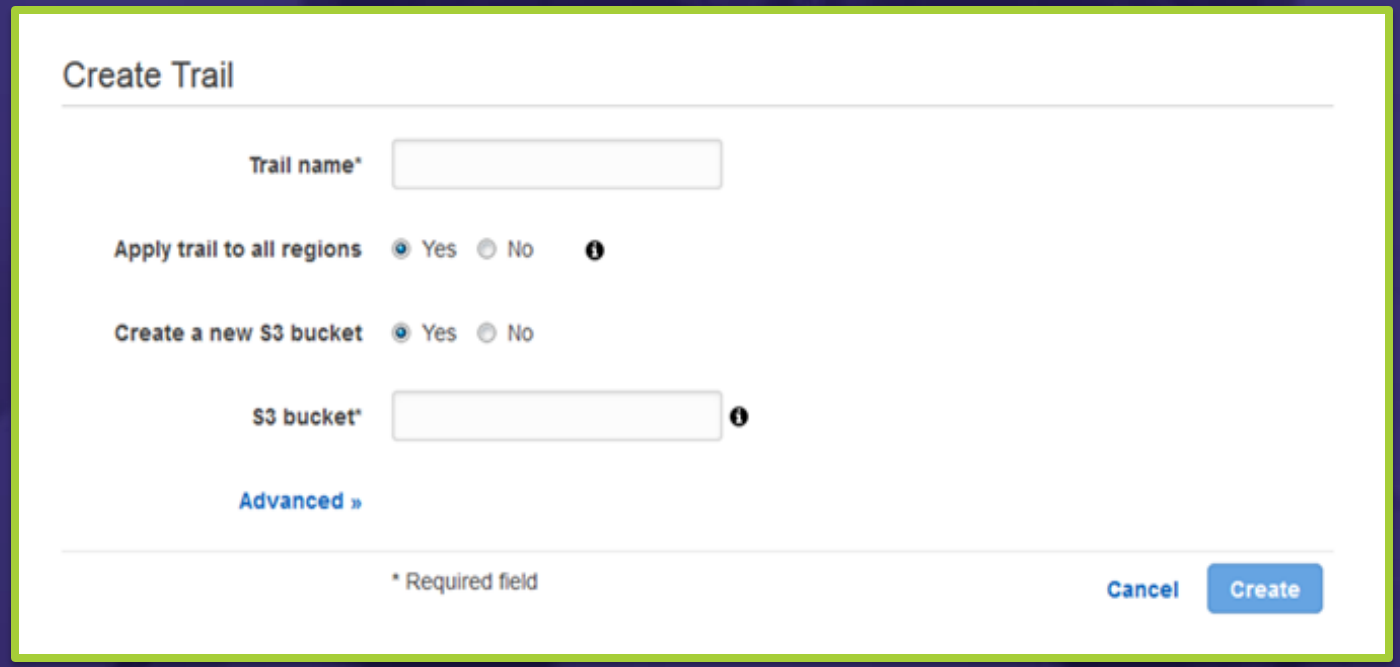
- Turned off by default
- Retention time, regions
- Log types, log content

## SaaS

- Doesn't always exist
- License tier
- Security logs vs. application logs

MITIGA

## Verify you have what you need



# Solution 1 : Visibility



## CSP

- Turned off by default
- Retention time, regions
- Log types, log content

## SaaS

- Doesn’t always exist
- License tier
- Security logs vs. application logs

MITIGA

# Solution 1 : Visibility

## CSP

- Turned off by default
- Retention time, regions
- Log types, log content

## SaaS

- Doesn't always exist
- License tier
- Security logs vs. application logs

MITIGA

## Contracts

| | Free | Pro | Business+ | Enterprise Grid |
|---|---|---|---|---|
| | | Upgrade Now | Upgrade Now | Contact Sales |
| Two-factor authentication | ✓ | ✓ | ✓ | ✓ |
| OAuth with Google | | ✓ | ✓ | ✓ |
| SAML-based single sign-on (SSO) | | | ✓ | Supports Multi-SAML |
| Slack Enterprise Key Management | | | | Add-on |
| Integration with Enterprise Mobility Management (EMM) | | | | ✓ |
| Audit logs | | | | ✓ |
| Identity provider (IDP) groups | | | | ✓ |

# Solution 1 : Visibility



## CSP

- Turned off by default
- Retention time, regions
- Log types, log content

## SaaS

- Doesn’t always exist
- License tier
- Security logs vs. application logs

MITIGA

# Problem 2 : Identity Over Malware

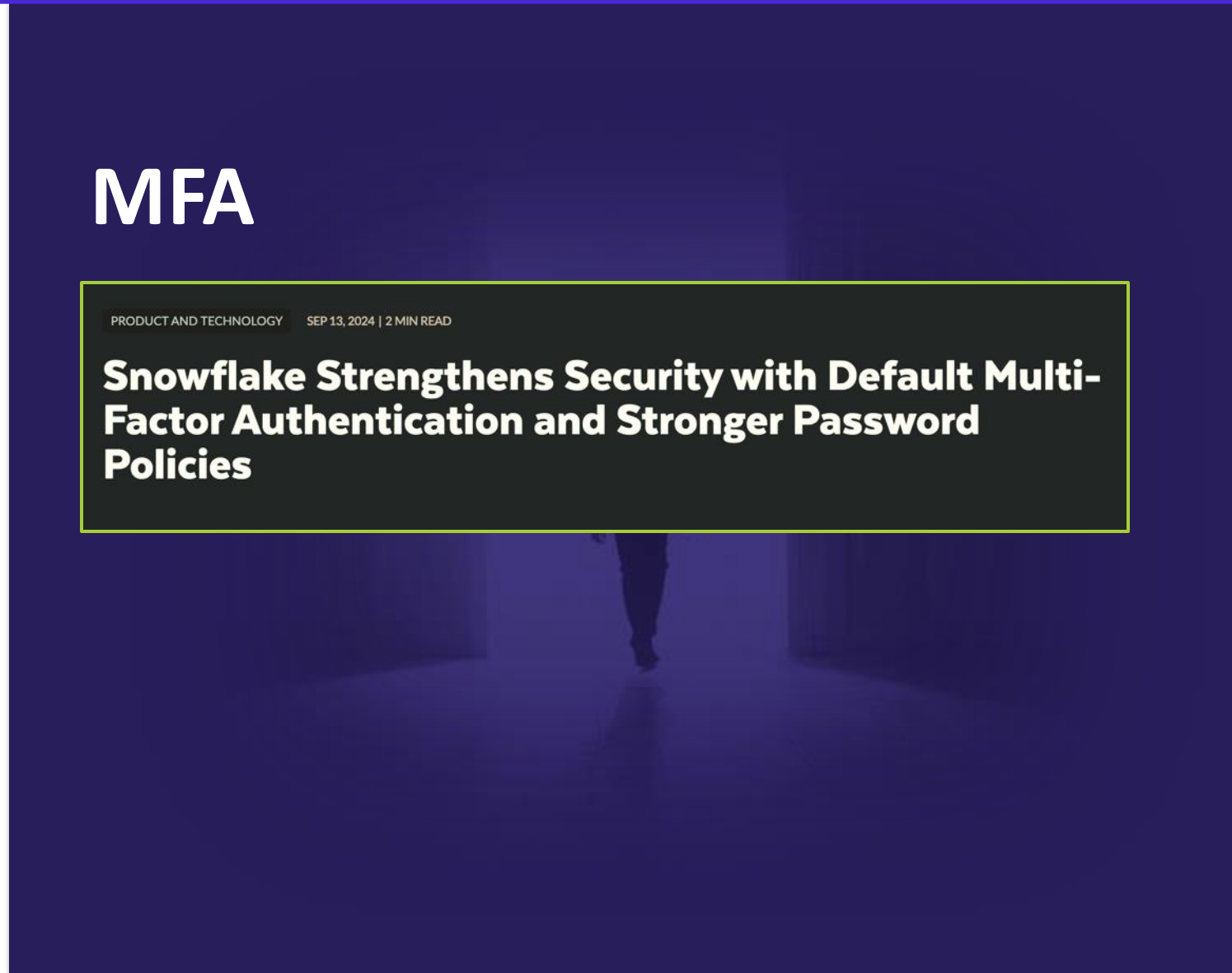


- No need for 0-day/n-day
- You can’t have hash for behavior
- InfoStealers are cheap and easy to use
- No more “Perimeter”

# Solution 2 : Identity Over Malware

- No need for 0-day/n-day
- You can’t have hash for behavior
- InfoStealers are cheap and easy to use
- No more “Perimeter”

## MFA


PRODUCT AND TECHNOLOGY
SEP 13, 2024 | 2 MIN READ
Snowflake Strengthens Security with Default Multi-Factor Authentication and Stronger Password Policies

MITIGA

# Solution 2 : Identity Over Malware



- No need for 0-day/n-day
- **You can't have hash for behavior**
- InfoStealers are cheap and easy to use
- No more "Perimeter"

## Characteristics

```
aws s3 sync s3://test-bucket /home/my-
destination-directorymc cp --recursive
s3/test-bucket.

s3cmd get --recursive s3://test-bucket
/home//s3-bucket/
```

MITIGA

# Solution 2 : Identity Over Malware

- No need for 0-day/n-day
- You can’t have hash for behavior
- **InfoStealers are cheap and easy to use**
- No more “Perimeter”

## Proactive Threat Intelligence Automation

# Solution 2 : Identity Over Malware



- No need for 0-day/n-day
- You can’t have hash for behavior
- InfoStealers are cheap and easy to use
- **No more “Perimeter”**

## Follow-up events

Disney Internal Slack | 1.1TiB
by NullBulge - Friday July 12, 2024 at 12:24 PM
bxby
Breached
MEMBER
Posts: 1
Threads: 0
Joined: Jul 2024
Reputation: 0
#21
NullBulge Wrote:
(Yesterday, 12:24 PM)
Hi there folks, it is us again.
Yesturday we leaked some small DB, now we leak the big guns.
1.1TiB of data. almost 10,000 channels, every message and file possible, dumped. Unreleased projects, raw images and code, some logins, links to internal api/web pages, and more! Have fun sifting through it, there is a lot there.
Perfect for gathering intelligence and more.
Bet they never imagined taking down ClubPenguin servers would cause this much shite

MITIGA

# Problem 3 : Skillset



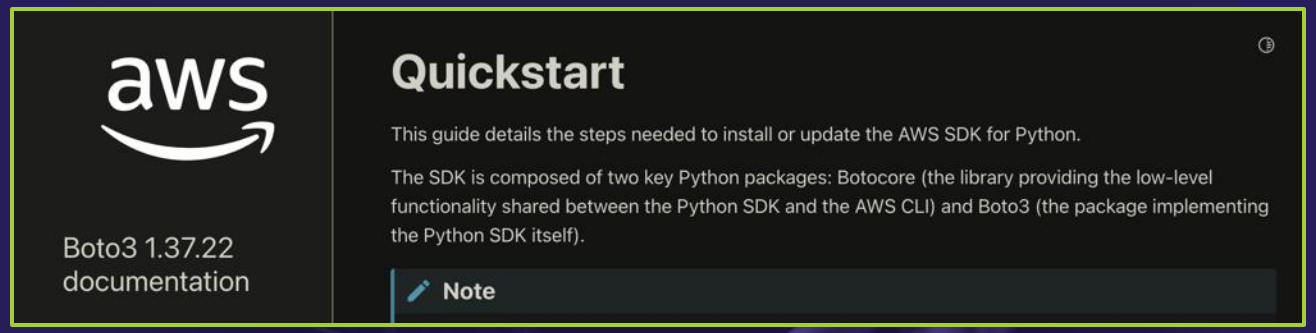
- Everything is over web and API
- How do you investigate a bucket “leak”?
- How to investigate HR SaaS after unauthorized login?
- No EDR for non-workload resources

MITIGA

# Solution 3 : Skillset

- Everything is over web and API
- How do you investigate a bucket “leak”?
- How to investigate HR SaaS after unauthorized login?
- No EDR for non-workload resources

## Training


aws
Boto3 1.37.22 documentation
Quickstart
This guide details the steps needed to install or update the AWS SDK for Python.
The SDK is composed of two key Python packages: Botocore (the library providing the low-level functionality shared between the Python SDK and the AWS CLI) and Boto3 (the package implementing the Python SDK itself).
Note

MITIGA

# Solution 3 : Skillset



- Everything is over web and API
- **How do you investigate a bucket “leak”?**
- How to investigate HR SaaS after unauthorized login?
- No EDR for non-workload resources

## Hands-on drills (Purple\Red)

# Solution 3 : Skillset



- Everything is over web and API
- How do you investigate a bucket “leak”?
- **How to investigate HR SaaS after unauthorized login?**
- No EDR for non-workload resources

## Ongoing internal Threat Hunting

MITIGA

# Solution 3 : Skillset



- Everything is over web and API
- How do you investigate a bucket “leak”?
- How to investigate HR SaaS after unauthorized login?
- **No EDR for non-workload resources**

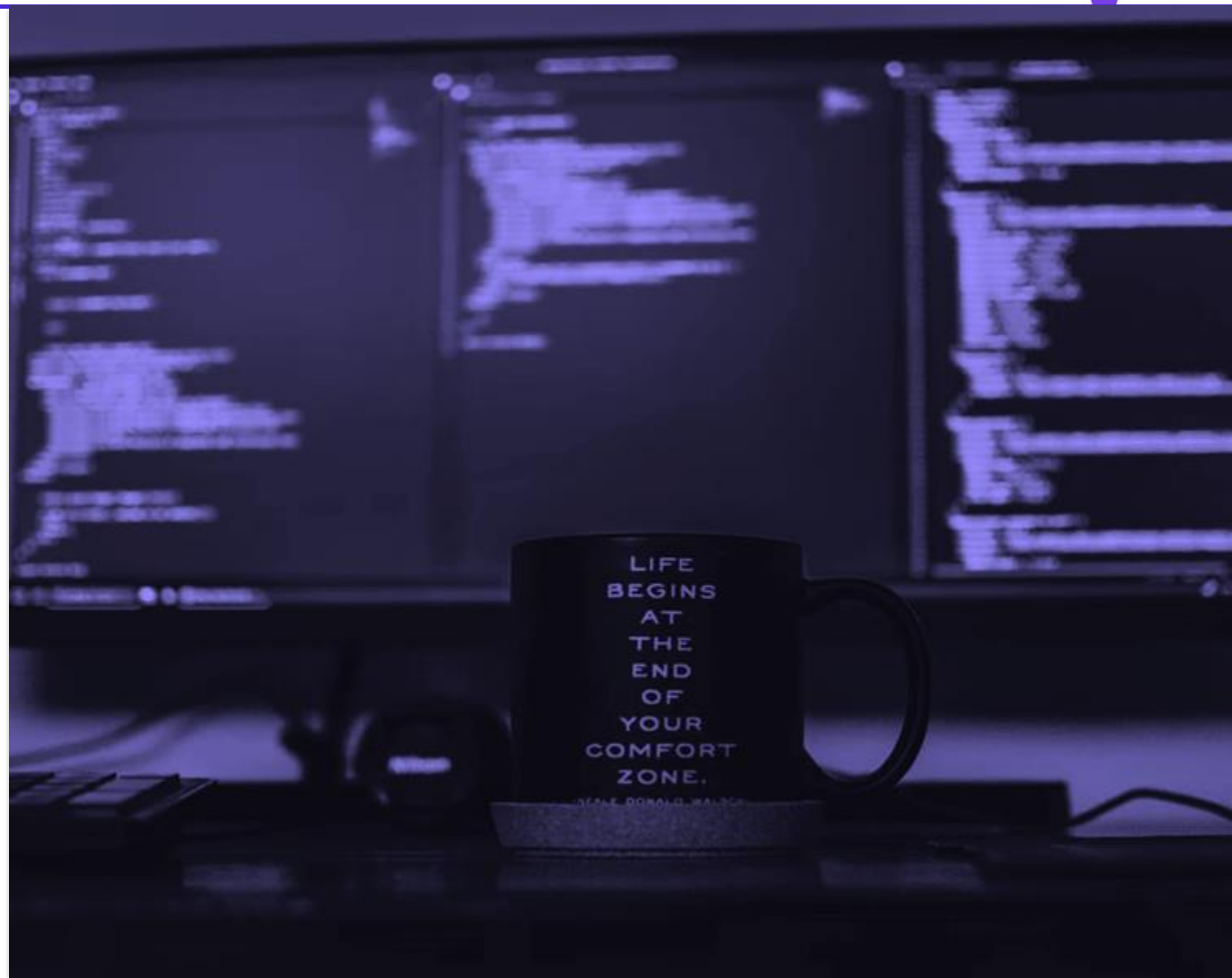
## Full monitoring for non-workload resources

MITIGA

# Problem 4 : RACI



- **Who owns Cloud Security/SaaS Security?**
  - Enabling logs?
  - Using logs?
  - Investigating?
  - Mitigating?

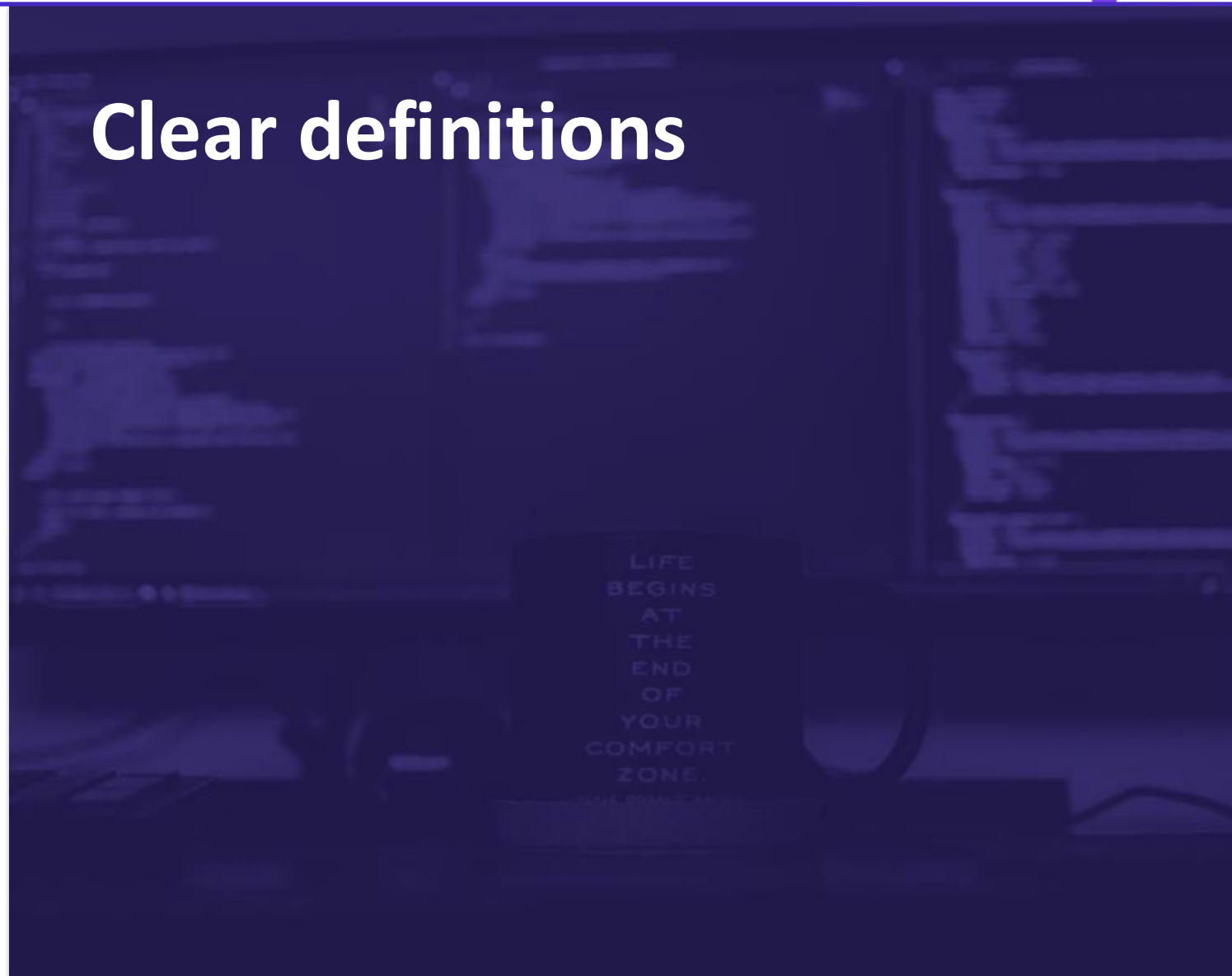



MITIGA

# Solution 4 : RACI



- **Who owns Cloud Security/SaaS Security?**
  - Enabling logs?
  - Using logs?
  - Investigating?
  - Mitigating?




MITIGA

# Solution 4 : RACI



- **Who owns Cloud Security/SaaS Security?**
  - Enabling logs?
  - Using logs?
  - Investigating?
  - Mitigating?

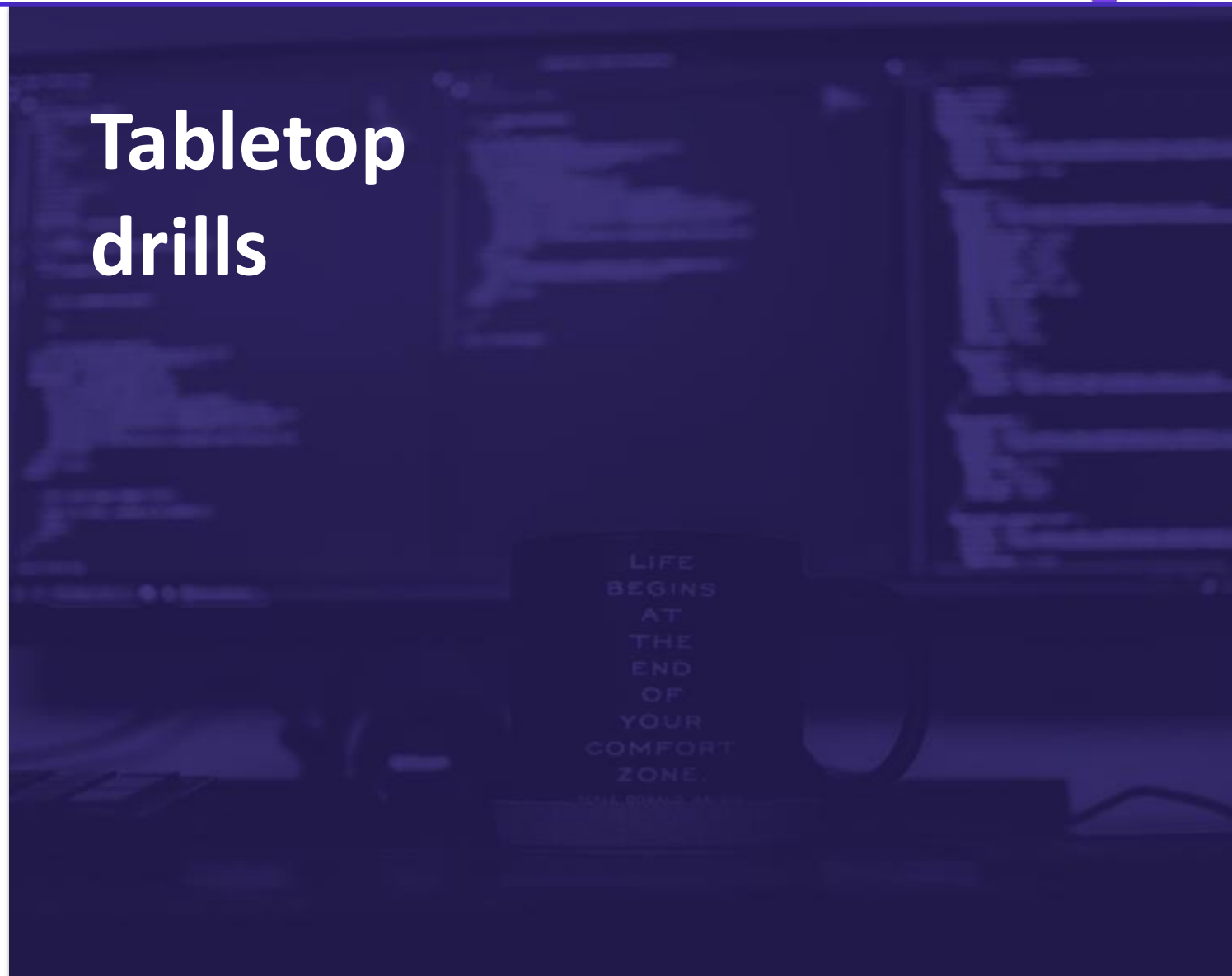
MITIGA

# Solution 4 : RACI



- **Who owns Cloud Security/SaaS Security?**
  - Enabling logs?
  - Using logs?
  - Investigating?
  - Mitigating?

## Tabletop drills




MITIGA

# Problem 5 : False Positives

- The age of Work from Anywhere
- Global companies
- Many SaaS
- Actions aren’t malicious – the intent is

# Solution 5 : False Positives

- The age of Work from Anywhere
- Global companies
- Many SaaS
- Actions aren’t malicious – the intent is

## How common are new things?

- New actions
- New platform
- New regions

# Solution 5 : False Positives

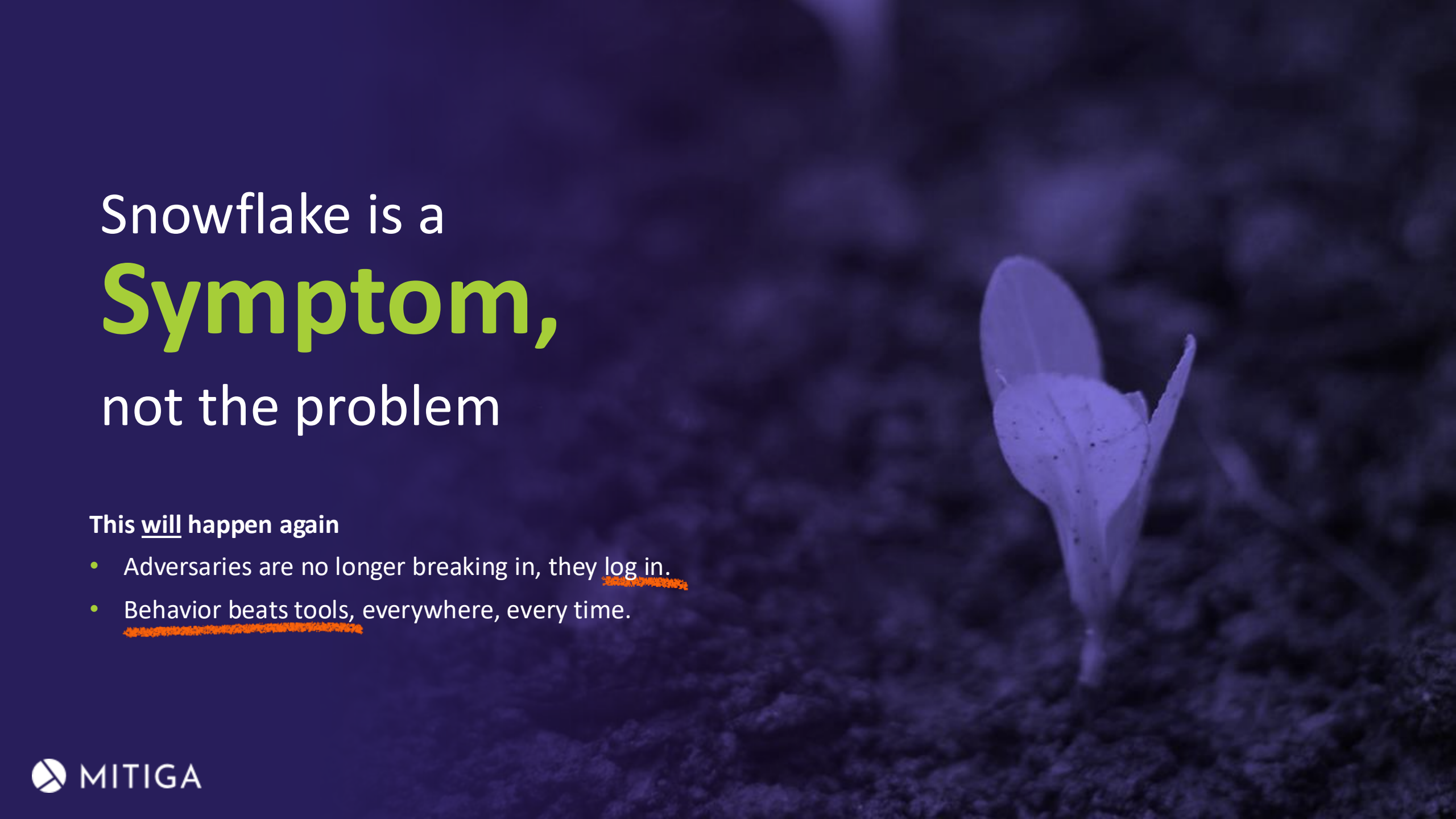


- The age of Work from Anywhere
- Global companies
- Many SaaS
- Actions aren’t malicious – the intent is

**Flow detection**

**v/s**

**Atomic detection**



# Snowflake is a **Symptom,** not the problem

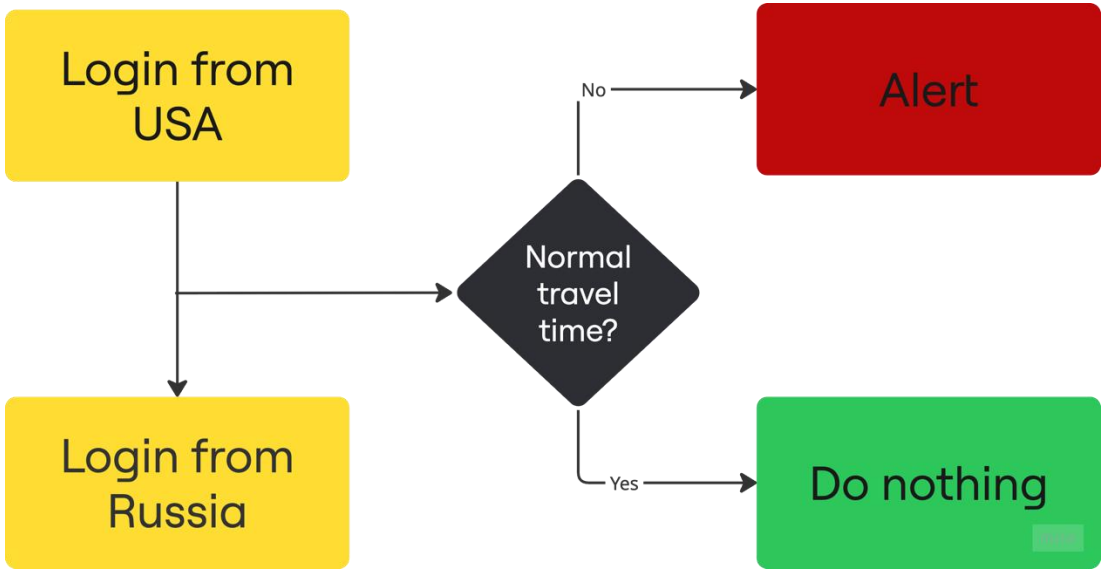
**This will happen again**

- Adversaries are no longer breaking in, they log in.
- Behavior beats tools, everywhere, every time.

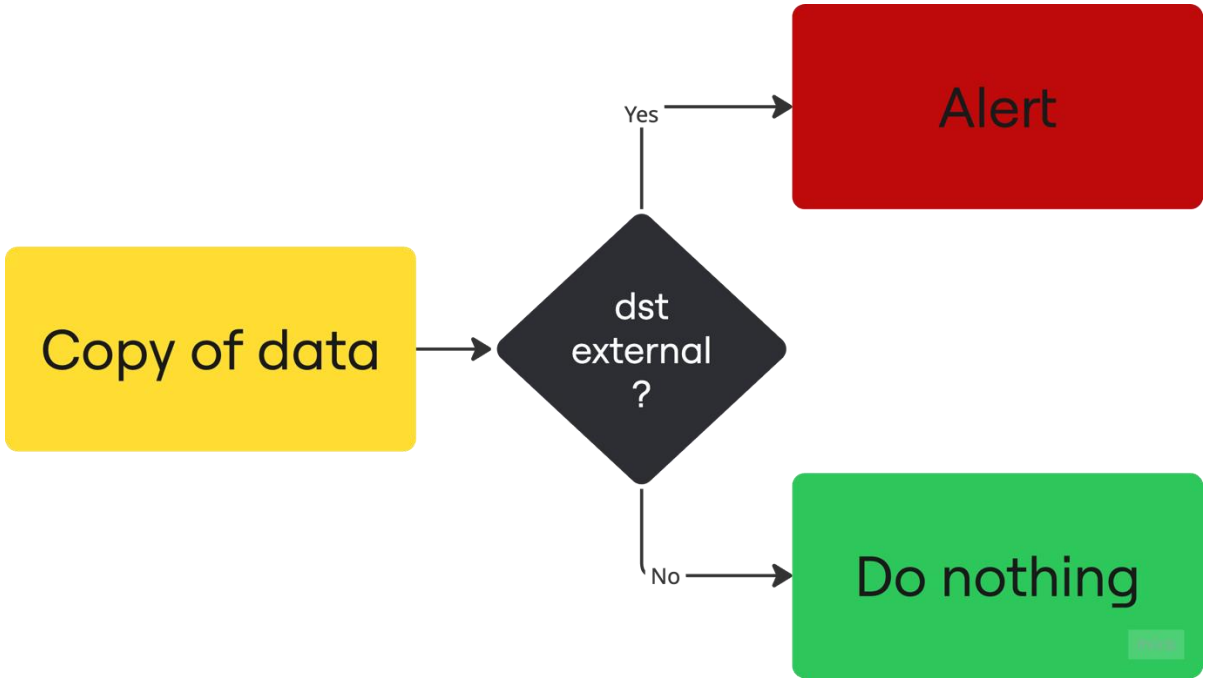
MITIGA

# Legacy Detection Examples

## IdP – Impossible Travel




## CSP - Data Exfiltration



# Advanced Detection Engineering



## Context-Aware, Behavioral and Anomaly-based

Where did they authenticate compared to usual?

Connection metadata – user-agent, OS, time

Is it a crown-jewel?

Do we have Threat Intelligence?

And more…!

# Behavioral Detection Engineering

**Threat Intelligence**

**Event Metadata**

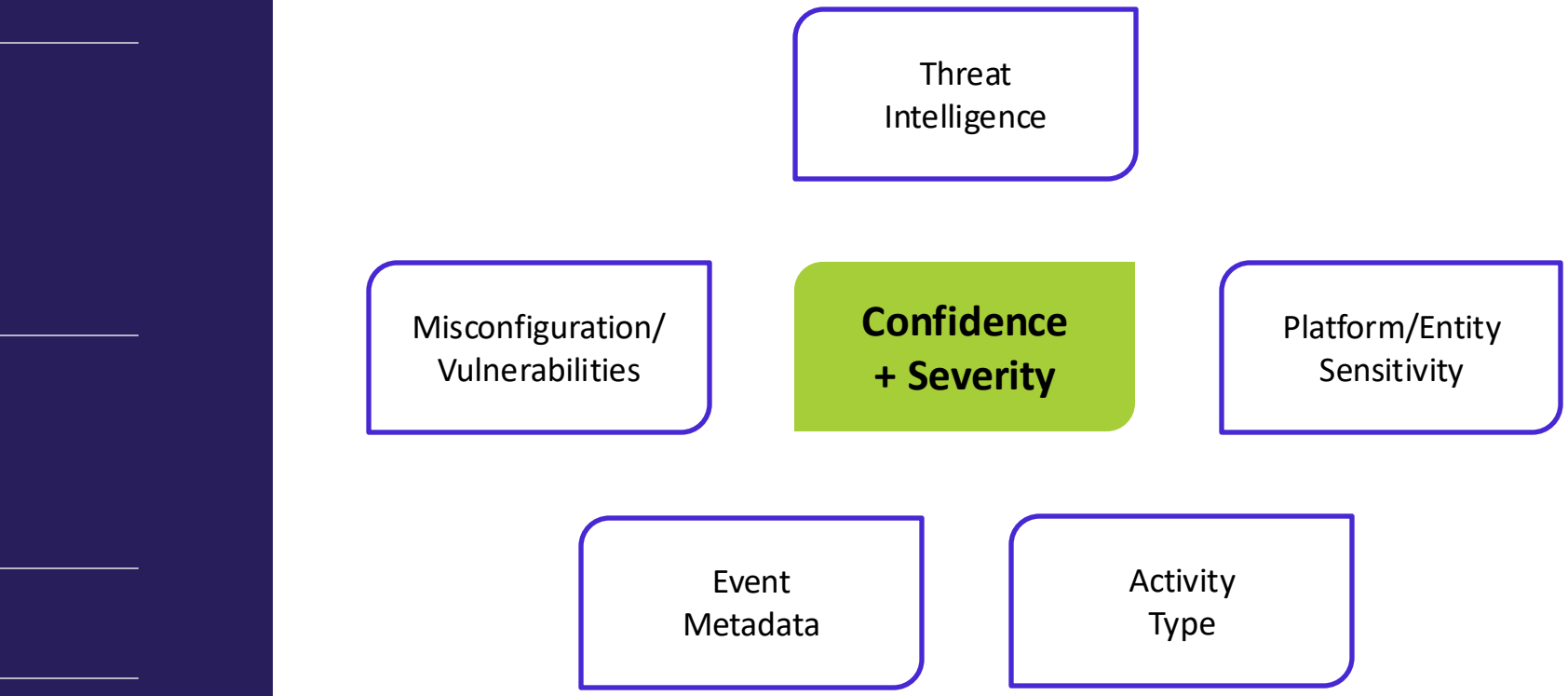
- Location, type (hosting, VPN, TOR)
- Time, Browser, OS
- Event-spike

**Activity type**

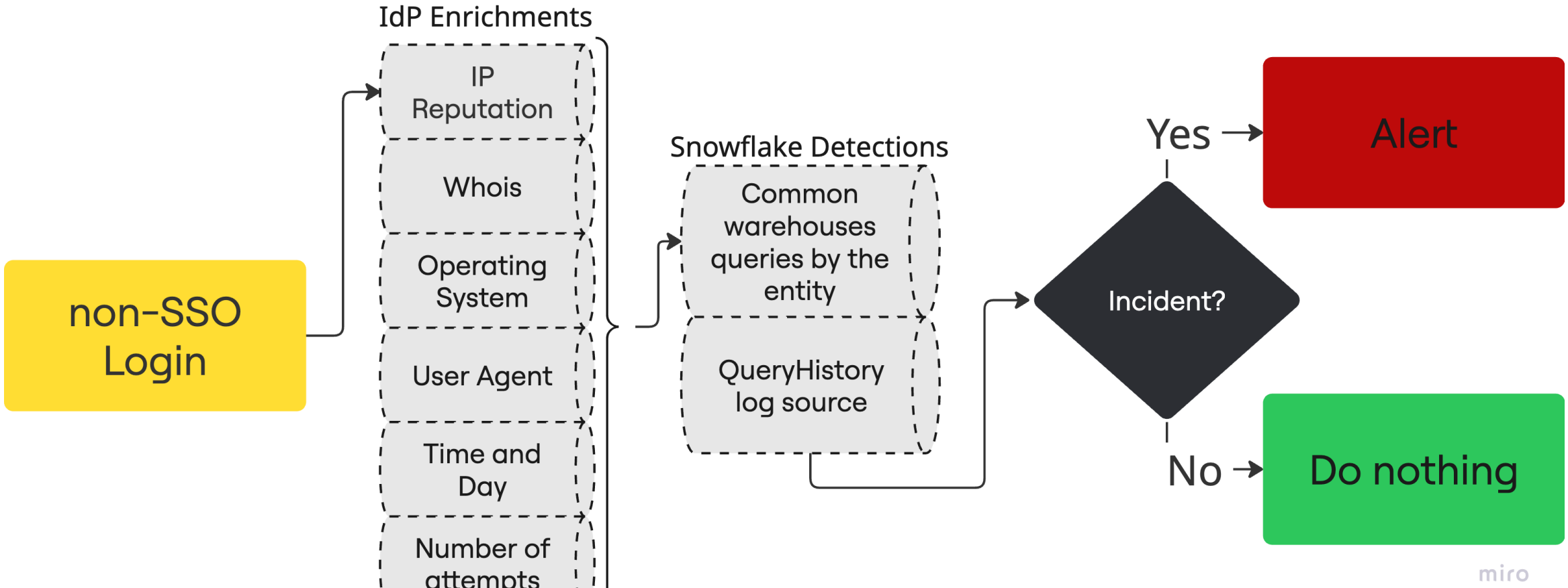
- Type of action
- Platform and/or region

**Platform/Entity sensitivity**

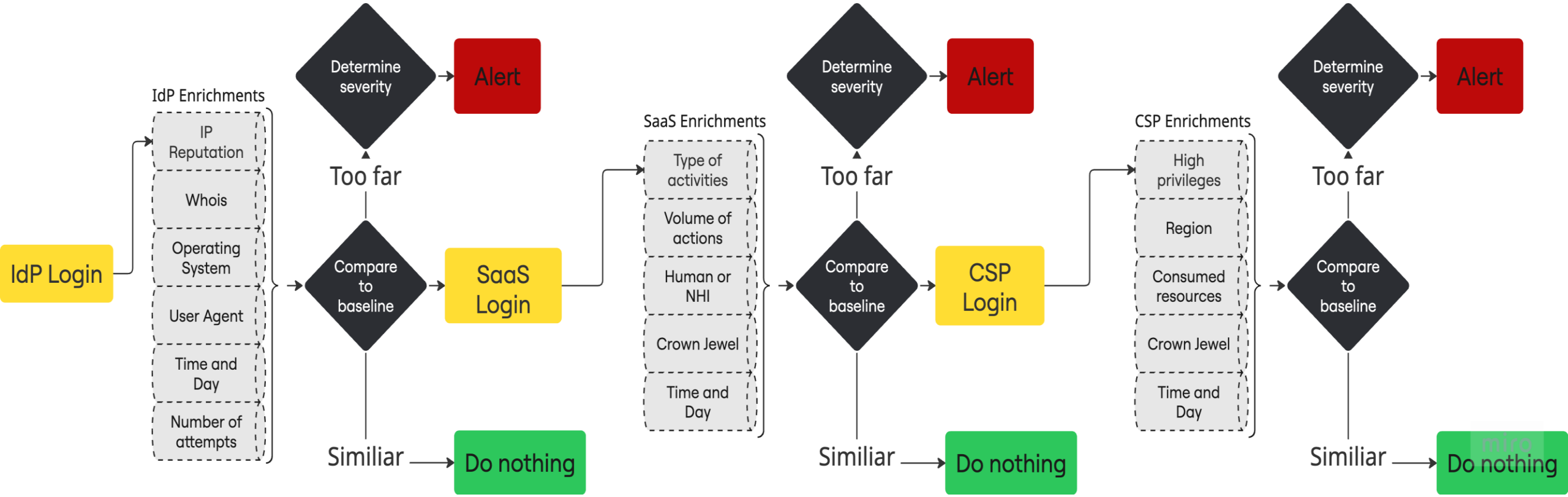
**Misconfiguration and/or vulnerabilities**



# Something is Going on – Is it Malicious?



# Holistic Cloud Detection Example



# Apply What You Learned Today!

## Next Week

### Increase your cloud visibility

- Verify you have adequate logs from your CSPs.
- Verify you have logs from all SaaS platforms.

## Next Month

### Plan forward

- Develop behavioral detection strategy
- Establish clear RACI for cloud security
- Invest in ongoing upskilling and threat detection

## And then…

### Baselining

- Collect and analyze logs from all systems to establish a baseline of normal activity over time.
- Implement anomaly detection tools to compare current logs against the baseline and alert on deviations.

MITIGA

RSAC 2025 Conference

RSAC™ 2025 Conference

Many Voices.
**One Community.**

# Thank You!